

# Manuale utente

v. 1.1.3

© 2006, Oberthur Card Systems. All rights reserved.

Le informazioni contenute in questa pubblicazione sono corrispondenti allo stato dell'arte della conoscenza di Oberthur Card System. In ogni caso, Oberthur Card Systems declina ogni responsabilità derivante dall'uso di queste informazioni e si riserva il diritto di cambiarle senza preavviso.

The information contained in this publication is accurate to the best Oberthur Card Systems knowledge. However, Oberthur Card Systems disclaims any liability resulting from the use of this information and reserves the right to make changes without notice.

# INDICE

|  |           |
|--|-----------|
| <b>PRESENTAZIONE DEL MANUALE.....</b>                        | <b>IV</b> |
| Scopo.....   | IV        |
| Destinatari.....   | IV        |
| Documenti collegati.....                                     | IV        |
| <b>CAPITOLO 1 – PRESENTAZIONE DI CNS MANAGER.....</b>        | <b>1</b>  |
| Cos'è CNS Manager?.....                                      | 1         |
| Scopo.....   | 1         |
| Elementi Principali.....                                     | 1         |
| Tipi di Certificati.....                                     | 1         |
| <b>CAPITOLO 2 – INSTALLAZIONE DI CNS MANAGER .....</b>       | <b>2</b>  |
| Requisiti di Sistema.....                                    | 2         |
| Hardware.....  | 2         |
| Software .....   | 2         |
| Installazione e rimozione di Web Pack .....                  | 2         |
| Installazione .....  | 2         |
| Rimozione .....  | 2         |
| Installazione di un Web Browser/Mailer.....                  | 3         |
| Tipi e Versioni di Browser/Mailer.....                       | 3         |
| Internet Explorer/Outlook .....                              | 3         |
| Mozilla Firefox .....  | 3         |
| Netscape Navigator/Messenger.....                            | 3         |
| <b>CAPITOLO 3 – USO DEL CNS MANAGER.....</b>                 | <b>4</b>  |
| Avvio e chiusura del CNS Manager .....                       | 4         |
| Avvio.....   | 4         |
| Finestra Principale - Illustrazione.....                     | 4         |
| Finestra Principale - Descrizione.....                       | 5         |
| Uscita.....  | 5         |
| Esportare un Certificato.....                                | 5         |
| Accesso Informazioni sulla carta.....                        | 6         |
| Informazioni Disponibili.....                                | 6         |
| Procedura.....   | 6         |
| Cambio del PIN di login .....                                | 6         |
| Cambio del PIN di firma.....                                 | 7         |
| Sblocco del PIN di Login.....                                | 8         |
| Sblocco del PIN di Firma .....                               | 9         |
| <b>CAPITOLO 4 – USO DEL WEB BROWSER con CNS MANAGER.....</b> | <b>10</b> |
| Argomenti Principali.....                                    | 10        |
| Requisiti Tecnici.....                                       | 10        |
| Configurazione del Browser.....                              | 10        |
| Internet Explorer.....                                       | 10        |
| Mozilla FireFox.....   | 10        |
| Netscape Navigator.....                                      | 10        |
| Lettura dei Certificati.....                                 | 11        |
| Internet Explorer.....                                       | 11        |
| Mozilla FireFox .....  | 12        |

|  |           |
|--|-----------|
| Netscape Navigator.....  | 13        |
| Autenticazione WEB .....   | 15        |
| Internet Explorer.....   | 15        |
| Mozilla FireFox .....  | 16        |
| Netscape Communicator.....   | 18        |
| <b>CAPITOLO 5 – PRESENTAZIONE DI BIT4ID Middleware Universale.....</b>         | <b>19</b> |
| Cos'è BIT4ID Middleware Universale?.....                                       | 19        |
| Scopo.....   | 19        |
| Elementi Principali.....   | 19        |
| Tipi di Certificati.....   | 19        |
| <b>CAPITOLO 6 – INSTALLAZIONE DI BIT4ID Middleware Universale.....</b>         | <b>20</b> |
| Requisiti di Sistema.....  | 20        |
| Hardware.....  | 20        |
| Software .....   | 20        |
| Installazione e rimozione di Web Pack .....                                    | 20        |
| Installazione .....  | 20        |
| Rimozione .....  | 20        |
| Installazione di un Web Browser.....   | 21        |
| Tipi e Versioni di Browser.....  | 21        |
| Internet Explorer/Outlook .....  | 21        |
| Mozilla Firefox .....  | 21        |
| <b>CAPITOLO 7 – USO DEL BIT4ID Middleware Universale.....</b>                  | <b>22</b> |
| Avvio e chiusura del BIT4ID Middleware Universale.....                         | 22        |
| Avvio.....   | 22        |
| Finestra Principale - Illustrazione.....                                       | 23        |
| Finestra Principale - Descrizione.....   | 24        |
| Uscita.....  | 24        |
| Esportare un Certificato.....  | 24        |
| Accesso Informazioni sulla carta.....  | 24        |
| Accesso Informazioni sulla carta.....  | 24        |
| Procedura.....   | 25        |
| Cambio del PIN di login .....  | 26        |
| Sblocco del PIN di login .....   | 27        |
| <b>CAPITOLO 8 – USO DEL WEB BROWSER con BIT4ID Middleware Universale.....</b>  | <b>28</b> |
| Argomenti Principali.....  | 28        |
| Requisiti Tecnici.....   | 28        |
| Configurazione del Browser.....  | 28        |
| Internet Explorer.....   | 28        |
| Mozilla FireFox.....   | 28        |
| Lettura dei Certificati.....   | 28        |
| Internet Explorer.....   | 29        |
| Mozilla FireFox .....  | 30        |
| Autenticazione WEB .....   | 32        |
| Internet Explorer.....   | 32        |
| Mozilla FireFox .....  | 33        |
| <b>DOMANDE FREQUENTI .....</b>   | <b>35</b> |
| Explorer non visualizza i certificati presenti sulla carta. Cosa faccio? ..... | 35        |
| Qual è il nome dell'eseguibile corrispondente al "CNS Manager" .....           | 35        |
| Qual è la directory di installazione del CNS Manager .....                     | 35        |
| Mozilla non visualizza i certificati presenti sulla carta. Cosa faccio?.....   | 35        |

|                                   |           |
|-----------------------------------|-----------|
| <b>GLOSSARIO.....</b>             | <b>36</b> |
| Autenticazione.....               | 36        |
| Certificato .....                 | 36        |
| Certification Authority (CA)..... | 36        |
| Decifratura.....                  | 36        |
| Firma Digitale .....              | 36        |
| Cifratura.....                    | 36        |
| Extranet .....                    | 37        |
| Intranet .....                    | 37        |
| Non ripudio .....                 | 37        |
| Chiave privata .....              | 37        |
| Chiave pubblica.....              | 37        |
| Algoritmo a chiave pubblica ..... | 37        |
| RSA.....                          | 37        |
| Smart Card.....                   | 37        |

# PRESENTAZIONE DEL MANUALE

## Scopo

Questo manuale:

- spiega come installare l'applicazione CNS Manager.
- Descrive le caratteristiche funzionali di CNS Manager (smart card e applicazioni CNS Manager).

## Destinatari

Questo manuale è destinato ai cittadini che vogliono usare CNS Manager per eseguire comunicazioni elettroniche, transazioni e commercio in sicurezza.

## Documenti collegati

Leggere la guida per l'installazione dei lettori per saperne di più sui lettori che possono essere associati al CNS Manager e sulle modalità della loro installazione.

# CAPITOLO 1 – PRESENTAZIONE DI CNS MANAGER

## Cos'è CNS Manager?

### Scopo

CNS Manager è una soluzione completa che permette di eseguire in sicurezza comunicazioni elettroniche e transazioni on-line utilizzando la smart card “Carta Nazionale dei Servizi”. Firme digitali, crittografie e certificati digitali assicurano l'autenticazione, il controllo degli accessi e la riservatezza.

L'insieme, carta CNS e CNS manager, è un passo verso la realizzazione dell'e-governement, cioè l'utilizzo delle nuove tecnologie dell'informazione e della comunicazione (ICT) per rendere la Pubblica Amministrazione sempre più veloce, efficiente e vicina al cittadino.

### Elementi Principali

Gli elementi principali di CNS Manager sono:

- Gestione certificati
- Gestione PIN Login (cambio e sblocco)
- Gestione PIN Firma (cambio e sblocco)
- Autenticazione Web per aprire un canale sicuro SSL.
- Operazioni di browser (invio e ricezione di mail firmate e/o criptate)

## Tipi di Certificati

Differenti certificati possono essere utilizzati con il CNS Manager. Un certificato è il passaporto digitale che contiene la chiave pubblica dell'utente ed è usato per:

- Autenticare il mittente
- Verificare l'integrità dei dati
- Provvedere al non ripudio dei dati
- Cifrare i dati spediti al possessore del certificato

Il certificato presente sulla CNS è un certificato di Autenticazione.

## CAPITOLO 2 – INSTALLAZIONE DI CNS MANAGER

Per utilizzare al meglio CNS Manager, l'hardware ed il software del vostro sistema devono rispondere ai seguenti requisiti:

### Requisiti di Sistema

Per utilizzare il CNS Manager è necessario avere a disposizione una CNS Oberthur C.S. che è una carta nazionale dei servizi conforme alle specifiche dettate dal CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione) nel documento "CNS – Carta Nazionale dei Servizi – Functional Specification v.1.1.2"

### Hardware

- Processore Pentium
- 32 MB RAM (si consiglia 64 MB)
- 3 MB di spazio disponibile sul disco, dipendenti dalla configurazione
- 5 MB di spazio libero temporaneamente per l'installazione
- Un lettore Smart Card correttamente installato

### Software

- Windows 98, 2000, NT con Service Pack 3 o successivo, XP
- Microsoft Internet Explorer 6.0, Mozilla Firefox 1.5, Netscape 7.1 o successivi
- Netscape Messenger 4.7.x o Microsoft Outlook 2000 o Express

### Installazione e rimozione di Web Pack

#### Installazione

Per installare il CNS Manager, si proceda come segue:

1. Uscire da tutti i programmi Windows
2. Inserire il CD-ROM nel lettore CD
3. Cliccare su Setup.exe
4. Seguire le istruzioni per l'installazione del programma.

#### Rimozione

Per rimuovere il CNS Manager, si proceda come segue:

1. Accedere al Pannello di Controllo e cliccare su Aggiungi/Rimuovi Programmi.
2. Selezionare CNS Manager dalla lista e cliccare Add/Delete.
3. Cliccare Yes per confermare.
4. Uscire dal Pannello di Controllo.

## Installazione di un Web Browser

### Tipi e Versioni di Browser/Mailer

Per utilizzare CNS Manager, è necessario installare uno dei seguenti Web browsers/mailers:

- Microsoft Internet Explorer 6.0 o successive e Outlook 2000 o Express
- Mozilla Firefox 1.5
- Netscape Navigator and Messenger 4.7 o successivo

### Internet Explorer/Outlook

Per installare Internet Explorer/Outlook, andare su <http://www.microsoft.com>. Seguire le istruzioni onscreen per effettuare il download ed installare il pacchetto.

### Mozilla Firefox

Per installare Internet Explorer/Outlook, andare su <http://www.mozilla.com/>. Seguire le istruzioni onscreen per effettuare il download ed installare il pacchetto.

### Netscape Navigator/Messenger

Per installare Netscape Navigator/Messenger, andare su <http://home.netscape.com>. Seguire le istruzioni on-screen per effettuare il download ed installare il pacchetto

<sup>1</sup>Indirizzo web corretto al momento della pubblicazione del manuale.




## CAPITOLO 3 – USO DEL CNS MANAGER

Nel presente capitolo sono trattati i seguenti aspetti:

- Avvio e chiusura del CNS Manager
- Esportazione certificato
- Accesso alle informazioni della carta
- Cambio del PIN di login
- Cambio del PIN di firma
- Sblocco del PIN di login
- Sblocco del PIN di firma


### Avvio e chiusura del CNS Manager

Quando la procedura di installazione è stata completata, selezionare **Start / Programs / CNS Manager / CNS Manager**

A questo punto l'applicazione gira in background e appare l'icona  nel system tray (pannello a sinistra dell'orologio).

#### Avvio

Per avviare CNS manager, procedere come segue:

1. Inserire la carta CNS nel lettore.
2. Cliccare con il tasto destro l'icona  e selezionare CNS Manager. Il lettore legge la carta e appare la finestra di login.
3. Inserire il pin di login e cliccare il pulsante Log in.

#### Finestra Principale - Illustrazione

Dopo aver inserito il pin di login, appare la seguente finestra principale:



## Finestra Principale – Descrizione

La finestra principale comprende quattro tabs come descritto sotto:

| Tab                         | Descrizione   |
|-----------------------------|---|
| Informazioni                | Fornisce le informazioni sulla smart card. Per ulteriori informazioni, si veda al paragrafo intitolato <a href="#">Ricerca Informazioni sulla Carta</a> a pagina 6. |
| PIN                         | Consente di cambiare il proprio PIN di login. Per ulteriori dettagli, si veda il paragrafo intitolato <a href="#">Cambio del PIN di Login</a> a pagina 6.           |
| PIN di firma                | Consente di cambiare il proprio PIN di firma. Per ulteriori dettagli, si veda il paragrafo intitolato <a href="#">Cambio del PIN di Firma</a> a pagina 6.           |
| Carta nazionale dei servizi | Permette di visualizzare il contenuto della carta.  |

## Uscita

| Se si vuole...  | Si deve...  |
|---|---|
| Uscire dalla finestra principale, ma lasciare CNS Manager nel system tray | Cliccare la crocetta nera nell'angolo in alto a destra della finestra.  |
| Chiudere CNS Manager  | Consente di cambiare il proprio PIN di login. Per ulteriori dettagli, si veda il paragrafo intitolato <a href="#">Cambio del PIN di Login</a> a pagina 6. |

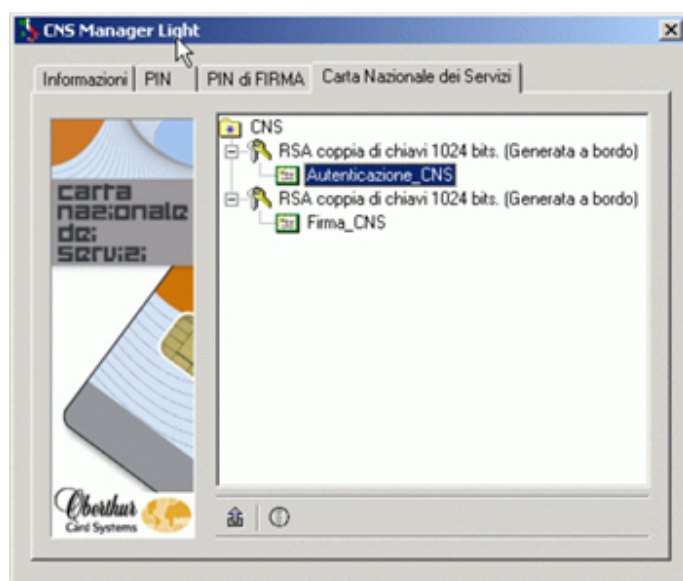
## Esportare un Certificato

Se un certificato è presente sulla carta e si lo si vuole utilizzare ad esempio per un'altra applicazione, lo si può esportare dalla carta alla corrispondente directory sul proprio sistema.

Per fare ciò, si proceda come segue:

1. Aprire la finestra principale e selezionare il tab Carta Nazionale dei Servizi.
2. Cliccare due volte la cartella principale e cliccare con il tasto sinistro la/e icona/e + vicina/e agli items per espandere la struttura.
3. Cliccare con il tasto sinistro il certificato da esportare.

Il certificato è evidenziato:



4. Cliccare l'icona Esporta il certificato selezionato, come indicato sopra.
  5. Sulla schermata successiva, selezionare la directory di destinazione, inserire un nome per il certificato e successivamente cliccare **Salva**.
- Il certificato è stato esportato nella directory prescelta, e si ritorna alla finestra principale.

## Accesso Informazioni sulla carta

Questa sezione descrive come accedere alle informazioni sulla smart card.

### Informazioni Disponibili

Le seguenti informazioni sono disponibili, come descritto sotto:

| Campo (Field)       | Definisce...                             |
|---------------------|--|
| Label               | Nome della smart card inserita           |
| Model               | Modello della smart card inserita.       |
| Manufacturer        | Estremi del produttore della smart card. |
| Serial number       | Numero seriale della smart card.         |
| Free memory         | Memoria disponibile in bytes.            |
| CNS Manager version | Versione di CNS Manager.                 |

### Procedura

Per accedere alle informazioni sulla smart card, entrare in CNS Manager come descritto nel paragrafo a pagina relativo.

Apparirà automaticamente il tab **Informazioni** sulla finestra principale.



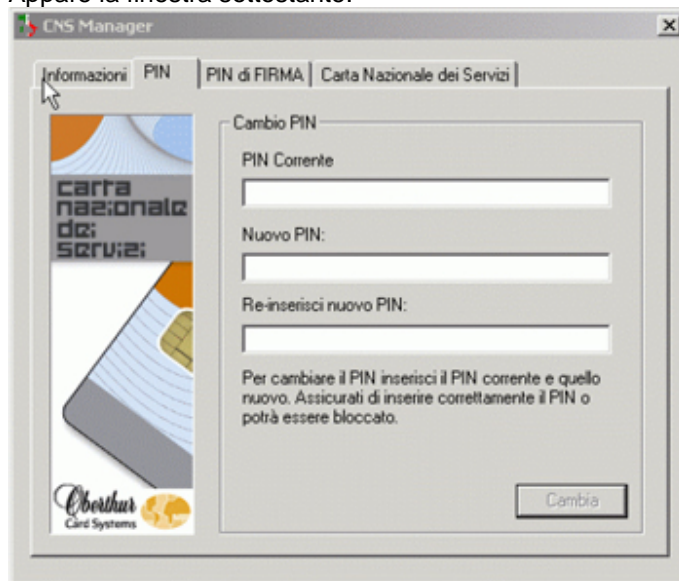
## Cambio del PIN di login

Per cambiare un PIN, si proceda nel modo seguente:

1. Aprire la finestra principale come descritto nel paragrafo a pagina intitolato Avvio

2. Cliccare il tab **PIN**.

Appare la finestra sottostante:



3. Inserire il PIN attuale nel campo **PIN Corrente**.
4. Inserire il nuovo PIN nel campo **Nuovo PIN**.
5. Confermare il nuovo PIN nel campo **Re-inserisci nuovo PIN**.
6. Cliccare **Cambia**.

Il nuovo PIN è stato applicato. Da questo momento dovrà essere utilizzato per effettuare il log in.

## Cambio del PIN di firma

Per cambiare un PIN di firma, si proceda nel modo seguente:

1. Aprire la finestra principale come descritto nel paragrafo intitolato Avvio

2. Cliccare il tab **PIN di firma**.  
Appare la finestra sottostante:

3. Inserire il PIN attuale nel campo **PIN Corrente**.
4. Inserire il nuovo PIN nel campo **Nuovo**.
5. Confermare il nuovo PIN nel campo **Re-inserisci nuovo**.
6. Cliccare **Cambia**.

Il nuovo PIN è stato applicato. Da questo momento dovrà essere utilizzato per effettuare il log in.

## Sblocco del PIN di Login

Nel caso in cui si sbagliasse per tre volte consecutive l'immissione del PIN di Login, per ragioni di sicurezza, la smart card blocca il PIN di login e il relativo accesso. Per sbloccare il PIN di login è necessario immettere un codice di sblocco chiamato PUK di login. Quando il PIN di Login è bloccato, il CNS Manager si presenta come segue:

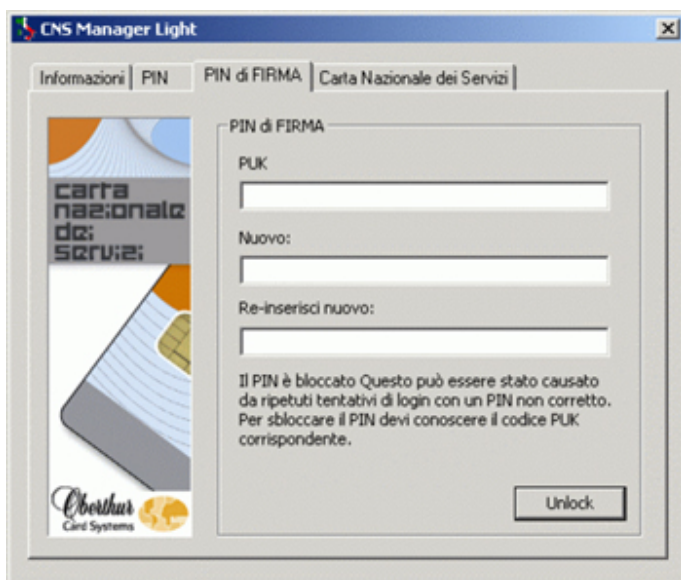
Per sbloccare il PIN, procedere come segue:

1. Digitare il PUK della carta CNS nella casella di testo PUK
2. Digitare un nuovo PIN (almeno 5 cifre) nella casella di testo Nuovo PIN
3. Ridigitare il PIN appena immesso nella casella di testo Reinserisci Nuovo PIN
4. Cliccare sul pulsante Unlock
5. Un messaggio conferma l'avvenuto sblocco del PIN di Login

**ATTENZIONE: Immettendo un PUK errato per tre volte consecutive, il PIN di Login viene definitivamente e irreversibilmente bloccato.**

## Sblocco del PIN di Firma

Nel caso in cui si sbagliasse per tre volte consecutive l'immissione del PIN di Firma, per ragioni di sicurezza, la smart card blocca il PIN Firma e il relativo accesso. Per sbloccare il PIN di Firma è necessario immettere un codice di sblocco chiamato PUK di Firma. Quando il PIN di Firma è bloccato, il CNS Manager si presenta come segue:



Per sbloccare il PIN di Firma, procedere come segue:

1. Digitare il PUK di Firma nella **casella di testo PUK**
2. Digitare un nuovo PIN di Firma (almeno 5 cifre) nella **casella di testo Nuovo PIN**
3. Ridigitare il PIN di Firma appena immesso nella **casella di testo Reinserisci Nuovo PIN**
4. Cliccare sul pulsante **Unlock**
5. Un messaggio conferma l'avvenuto sblocco del PIN di Login

**ATTENZIONE: Immettendo un PUK di Firma errato per tre volte consecutive, il PIN di Firma viene definitivamente e irreversibilmente bloccato, non sarà più possibile firmare dei documenti**

## CAPITOLO 4 – USO DEL WEB BROWSER con CNS MANAGER

In questo capitolo sono contenute tutte le informazioni necessarie per leggere il certificato sul browser e per firmare o cifrare e-mail in combinazione con CNS Manager.

### Argomenti Principali

In questo capito sono trattati i seguenti argomenti:

- Lettura del certificato con Netscape Navigator o Internet Explorer
- Autenticazione Web
- Firma e cifratura di email con Netscape Messenger o Microsoft Outlook

### Requisiti Tecnici

Sono richieste le seguenti versioni di browser e mailer:

- Internet Explorer 5.0 o successive e Outlook 2000 o Express
- Mozilla Firefox o successivi
- Netscape Navigator o Messenger 4.7.x o successivi

### Configurazione del Browser

#### Internet Explorer

Non è necessario fare nulla.

#### Mozilla FireFox

In questo paragrafo viene descritta la procedura da seguire per impostare Mozilla FireFox in modo che legga automaticamente i certificati contenuti nella CNS smart card. Procedere come segue:

1. Avviare Mozilla FireFox
2. Selezionare Apri File dal menu File
3. Selezionare il file "add\_profile\_CNS\_Oberthur.html" contenuto nella cartella di installazione (es. C:\Programmi\Oberthur Card Systems\CNS Manager)
4. Cliccare su Apri
5. Cliccare su OK ai messaggi che si presenteranno nel seguito

Volendo ripristinare la configurazione originale, eseguire la stessa procedura aprendo il file "remove\_profile\_CNS\_Oberthur.html".

#### Netscape Navigator

In questo paragrafo viene descritta la procedura da seguire per impostare Netscape Navigator in modo che legga automaticamente i certificati contenuti nella CNS smart card. Procedere come segue:



1. Avviare Netscape Navigator
2. Selezionare Apri File dal menu File
3. Selezionare il file "add\_profile\_CNS\_Oberthur.html" contenuto nella cartella di installazione (es. C:\Programmi\Oberthur Card Systems\CNS Manager)
4. Cliccare su Apri
5. Cliccare su OK ai messaggi che si presenteranno nel seguito

Volendo ripristinare la configurazione originale, eseguire la stessa procedura aprendo il file "remove\_profile\_CNS\_Oberthur.html".

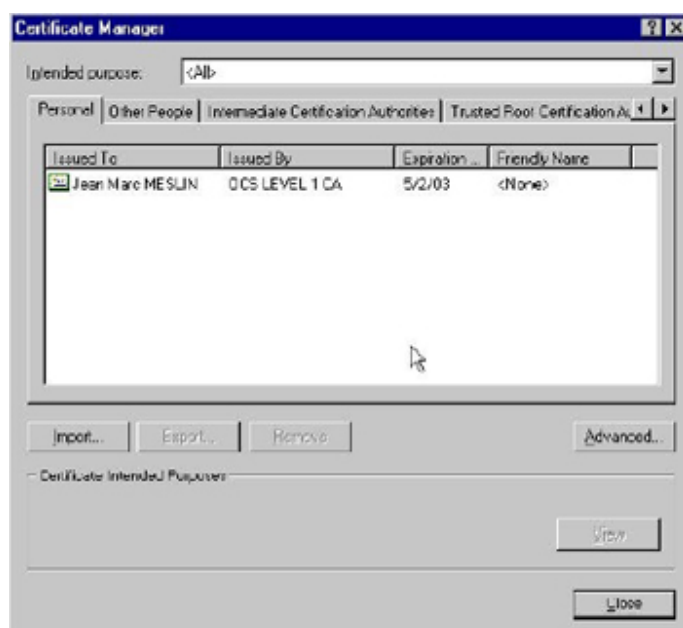
## Lettura dei Certificati

Questa sezione indica come leggere il certificato una volta che è stato installato sul browser. E' necessario installare il certificato solo su Netscape Navigator; non è necessaria una configurazione per Internet Explorer. Lo si può utilizzare per effettuare in sicurezza operazioni online.

## Internet Explorer

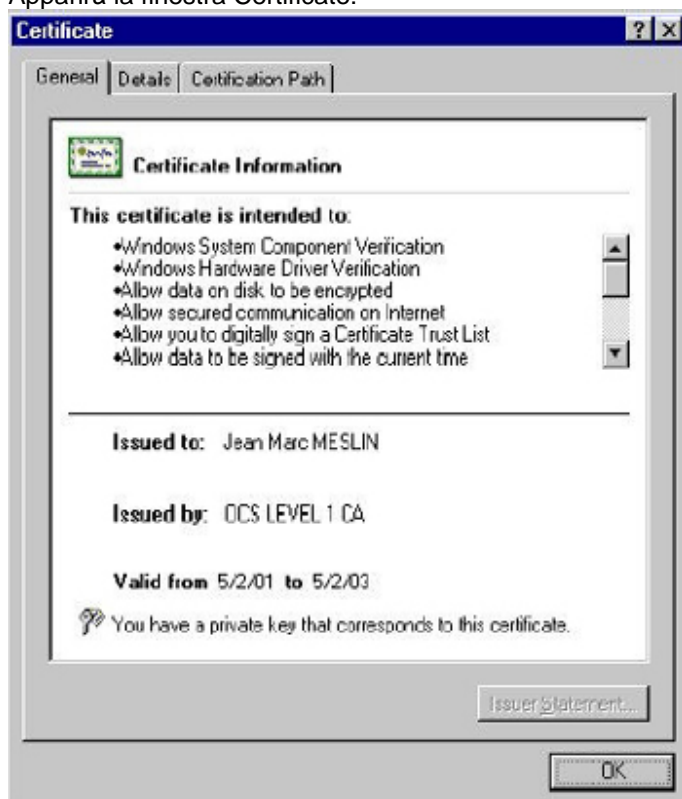
Per poter leggere un certificato su Internet Explorer, si proceda nel modo seguente:

1. Inserire la smart card CNS nel lettore.
2. Avviare Internet Explorer.
3. Nel menu **Strumenti**, cliccare **Opzioni Internet**.
4. Cliccare il tab **Contenuto**
5. Nell'area **Certificati**, cliccare il pulsante **Certificati** per vedere i certificati installati. Apparirà la finestra **Certificate Manager**:





6. Selezionare il certificato e cliccare View.  
Apparirà la finestra Certificate:



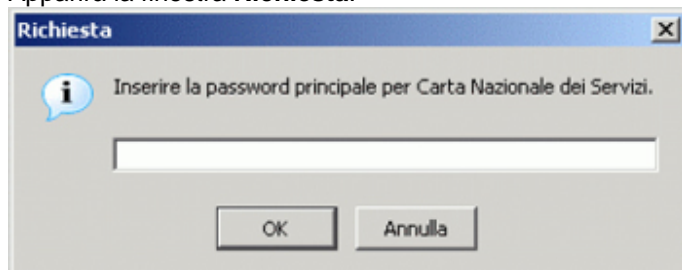
7. Cliccare OK, e, una volta terminato il tutto, Close.

## Mozilla FireFox

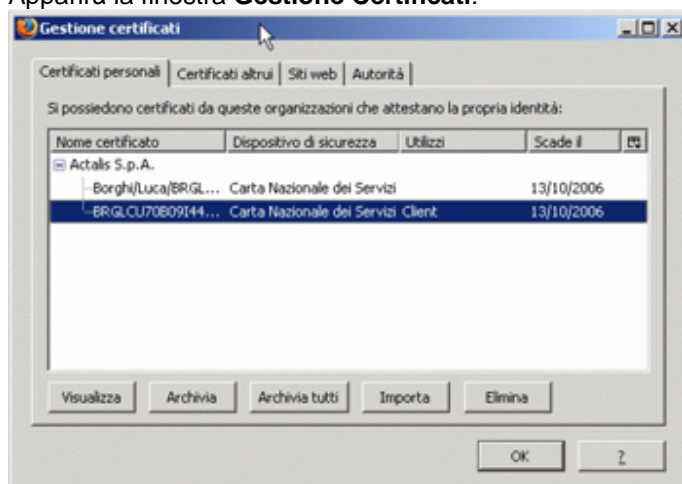
Per poter leggere un certificato su Mozilla FireFox, si proceda nel modo seguente:

1. Inserire la smart card CNS nel lettore.
2. Avviare Mozilla FireFox.
3. Selezionare **Strumenti, Opzioni**
4. Selezionare la sottofinestra **Avanzate**
5. Cercare la sezione **Certificati**
6. Cliccare sul pulsante **Gestione Certificati**

Apparirà la finestra **Richiesta**:



7. Inserire il PIN di Login e cliccare **OK**.  
Apparirà la finestra **Gestione Certificati**:



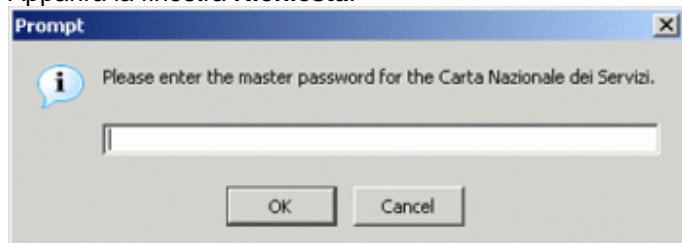
8. Selezionare il tab **Certificati personali**.
9. Cliccare con il tasto sinistro sul certificato corrispondente per selezionarlo e cliccare il pulsante **Visualizza**. Apparirà una descrizione dettagliata del certificato
10. Cliccare **OK** per chiudere

## Netscape Navigator

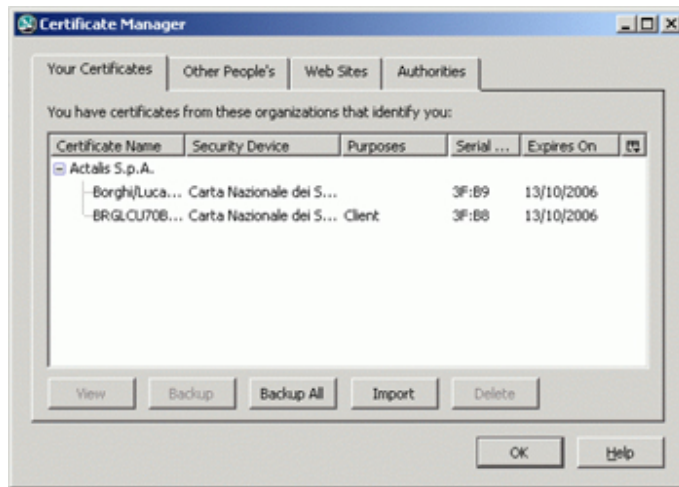
Per poter leggere un certificato su Netscape Navigator, si proceda nel modo seguente:

1. Inserire la smart card CNS nel lettore.
2. Avviare Netscape Navigator.
3. Selezionare Strumenti, Opzioni
4. Selezionare la sottofinestra Avanzate
5. Cercare la sezione Certificati
6. Cliccare sul pulsante Gestione Certificati

Apparirà la finestra **Richiesta**:



7. Inserire il PIN di Login e cliccare **OK**.  
Apparirà la finestra **Gestione Certificati**:



8. Selezionare il tab **Certificati Personali**
9. Cliccare con il tasto sinistro sul certificato corrispondente per selezionarlo e cliccare il pulsante **Visualizza**. Apparirà una descrizione dettagliata del certificato
10. Cliccare **OK** per chiudere

## Autenticazione WEB

La CNS smart card dispone di certificati che permettono l'autenticazione WEB. Normalmente i dati scambiati via internet sono "in chiaro" e un intruso potrebbe indebitamente accedere a informazioni confidenziali. E' possibile, tramite il protocollo SSL (Secure Socket Layer), stabilire un canale di comunicazione criptato e sicuro.

Oltre a questo primo livello di sicurezza, l'autenticazione web è un meccanismo che, grazie alla smart card CNS, permette al server web di assicurarsi dell'identità dell'utente che cerca di connettersi. Le informazioni riservate comunicate dal server web saranno protette per due ragioni:

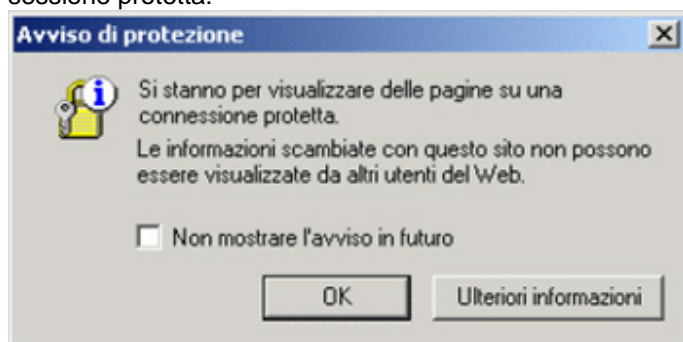
1. Sono criptate e firmate, quindi nessuno può né leggerle né modificarle
2. Sono trasmesse solo se l'utente è stato validamente identificato

IMP: Se non si importano i certificati delle certification authorities che hanno emesso il proprio certificato, il browser non permette l'uso dei certificati SSL client.

Qui di seguito la procedura da seguire per autenticarsi su richiesta di un server web che voglia stabilire una sessione SSL.

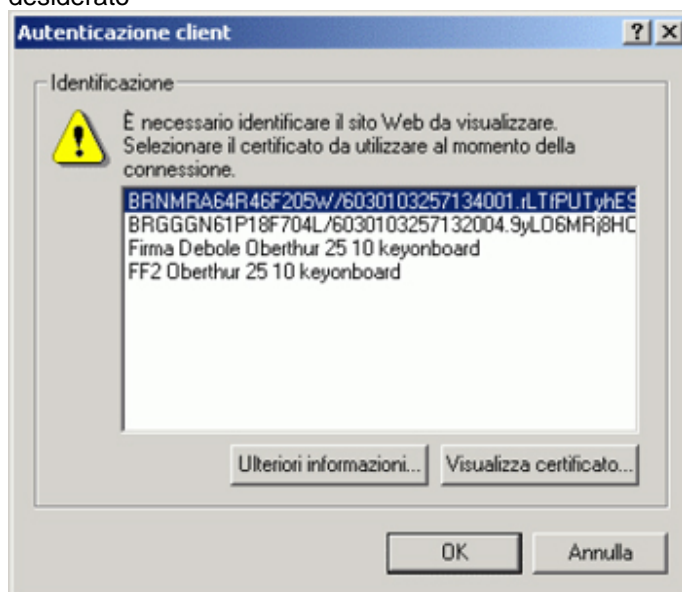
### Internet Explorer

Aperto una connessione sicura con un server web, Explorer avverte che si sta per aprire una sessione protetta:



Seguire la procedura specificata qui di seguito:

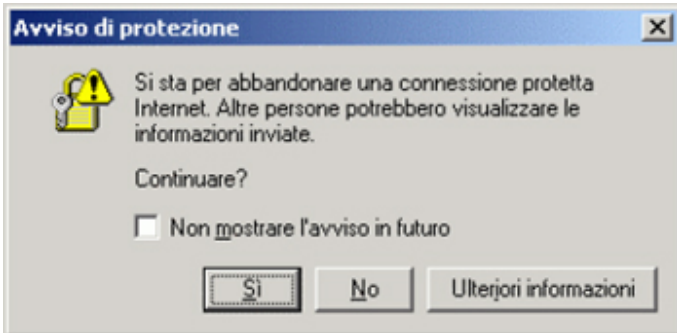
1. Cliccare su **OK**
2. Apparirà la finestra di **Autenticazione Client** dove poter scegliere il certificato di autenticazione desiderato



3. Scegliere il certificato di autenticazione desiderato e cliccare **OK**  
Apparirà la finestra di **Avviso di protezione**
4. Cliccare su **Si** (solo se la data del certificato è valida)

Da questo momento in avanti la connessione è sicura, cioè nessuno potrà leggere i dati intercorrenti tra server e client. Internet Explorer segnala lo stato di connessione sicura visualizzando nella sua status bar.

Terminando la connessione sicura, Microsoft Explorer visualizzerà la seguente finestra che avvisa il cambiamento di stato di connessione.

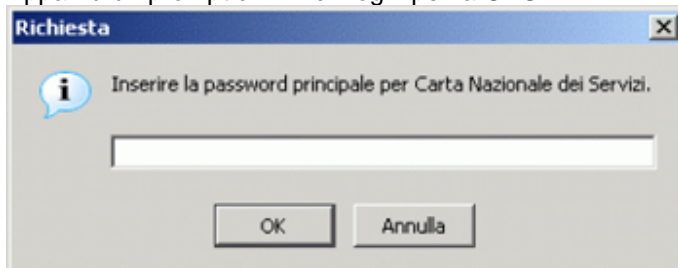


### Mozilla FireFox

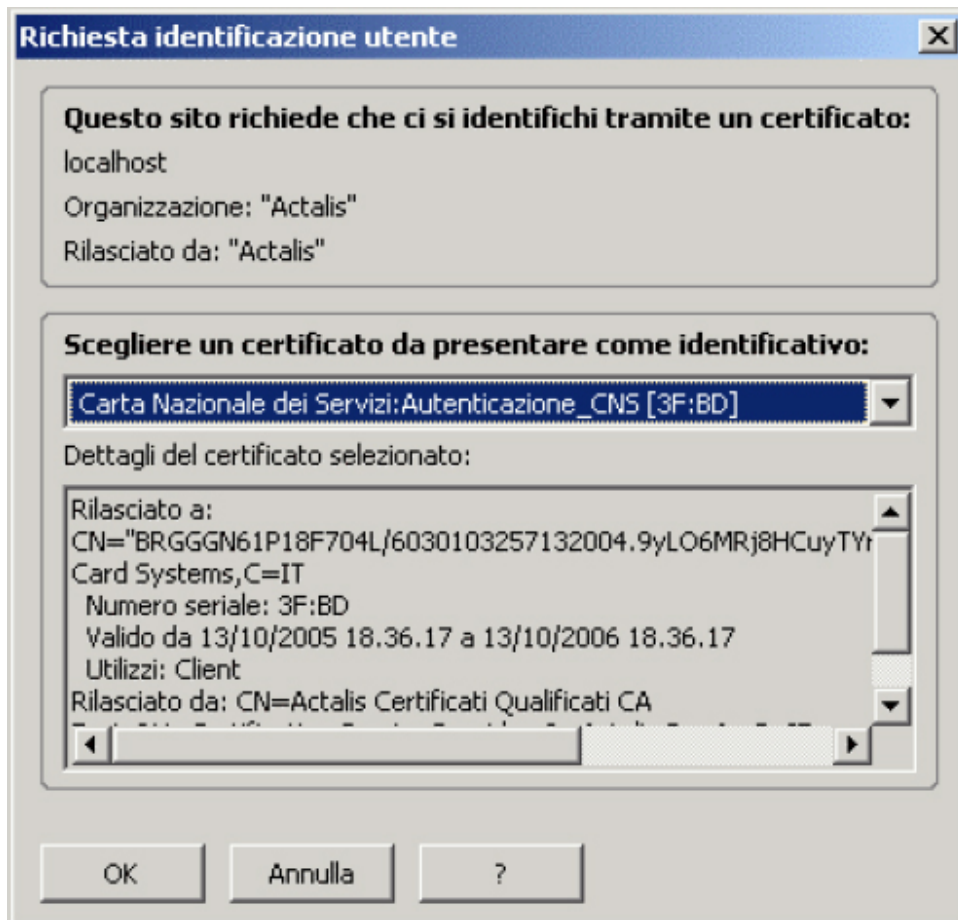
Aperto una connessione sicura con un server web, Mozilla FireFox avverte che si sta per aprire una sessione protetta.

Seguire la procedura specificata qui di seguito:


1. Apparirà un prompt di PIN di Login per la **CNS**:



2. Inserire il PIN di Login e cliccare su **OK**
3. Apparirà la finestra di **Richiesta identificazione Utente** dove poter scegliere il certificato di autenticazione desiderato



4. Scegliere il certificato di autenticazione desiderato e cliccare **OK**

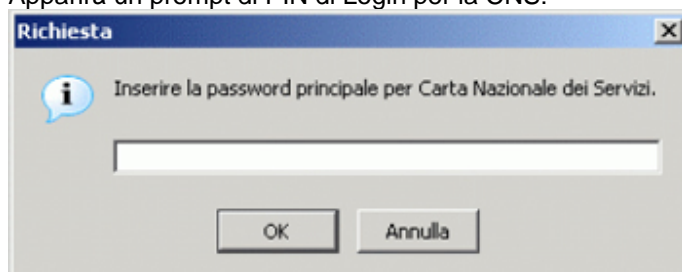
Da questo momento in avanti la connessione è sicura, cioè nessuno potrà leggere i dati intercorrenti tra server e client. Mozilla FireFox segnala lo stato di connessione sicura visualizzando  nella sua status bar e ombreggiando in giallo la barra degli indirizzi.

## Netscape Communicator

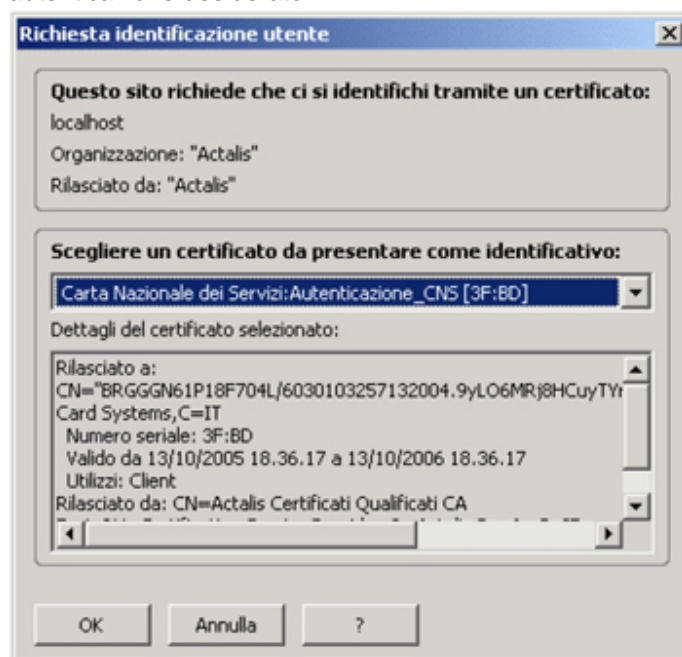
Aperto una connessione sicura con un server web, Netscape Communicator avverte che si sta per aprire una sessione protetta.

Seguire la procedura specificata qui di seguito:

1. Apparirà un prompt di PIN di Login per la CNS:



2. Inserire il PIN di Login e cliccare su **OK**
3. Apparirà la finestra di **Richiesta identificazione Utente** dove poter scegliere il certificato di autenticazione desiderato



4. Scegliere il certificato di autenticazione desiderato e cliccare **OK**

Da questo momento in avanti la connessione è sicura, cioè nessuno potrà leggere i dati intercorrenti tra server e client. Mozilla FireFox segnala lo stato di connessione sicura visualizzando nella sua status bar e ombreggiando in giallo la barra degli indirizzi.

## CAPITOLO 5 – PRESENTAZIONE DI BIT4ID Middleware Universale

### Cos'è BIT4ID Middleware Universale?

#### Scopo

BIT4ID Middleware Universale consente una semplice e piena integrazione nelle architetture a chiave pubblica per la firma digitale a validità legale, per l'autenticazione forte nell'accesso a servizi on-line.

#### Elementi Principali

Gli elementi principali di BIT4ID sono:

- Gestione certificati
- Gestione PIN Login (cambio e sblocco)
- Autenticazione Web per aprire un canale sicuro SSL.
- Operazioni di browser (invio e ricezione di mail firmate e/o criptate)

### Tipi di Certificati

Differenti certificati possono essere utilizzati con il BIT4ID. Un certificato è il passaporto digitale che contiene la chiave pubblica dell'utente ed è usato per:

- Autenticare il mittente
- Verificare l'integrità dei dati
- Provvedere al non ripudio dei dati

Il certificato presente sulla BIT4ID è un certificato di Autenticazione.



## CAPITOLO 6 – INSTALLAZIONE DI BIT4ID Middleware Universale

Per utilizzare al meglio BIT4ID, l'hardware ed il software del vostro sistema devono rispondere ai seguenti requisiti:

### Requisiti di Sistema

Per utilizzare il BIT4ID è necessario avere a disposizione una CNS Oberthur C.S. che è una carta nazionale dei servizi conforme alle specifiche dettate dal CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione) nel documento "CNS – Carta Nazionale dei Servizi – Functional Specification v.1.1.2"

#### Hardware

- Processore Pentium
- 32 MB RAM (si consiglia 64 MB)
- 3 MB di spazio disponibile sul disco, dipendenti dalla configurazione
- 5 MB di spazio libero temporaneamente per l'installazione
- Un lettore Smart Card correttamente installato

#### Software

- Windows 98, 2000, NT con Service Pack 3 o successivo, XP
- Microsoft Internet Explorer 6.0, Mozilla Firefox 1.5, Netscape 7.1 o successivi
- Netscape Messenger 4.7.x o Microsoft Outlook 2000 o Express

### Installazione e rimozione di Web Pack

#### Installazione

Per installare il BIT4ID Middleware Universale, si proceda come segue:

5. Uscire da tutti i programmi Windows
6. Inserire il CD-ROM nel lettore CD
7. Cliccare su Setup.exe
8. Seguire le istruzioni per l'installazione del programma.

#### Rimozione

Per rimuovere il BIT4ID Middleware Universale, si proceda come segue:

5. Accedere al Pannello di Controllo e cliccare su Aggiungi/Rimuovi Programmi.
6. Selezionare BIT4ID Middleware Universale dalla lista e cliccare Add/Delete.
7. Cliccare Yes per confermare.
8. Uscire dal Pannello di Controllo.

## Installazione di un Web Browser

### Tipi e Versioni di Browser/Mailer

Per utilizzare BIT4ID Middleware Universale, è necessario installare uno dei seguenti Web browsers/mailers:

- Microsoft Internet Explorer 6.0 o successive e Outlook 2000 o Express
- Mozilla Firefox 1.5

### Internet Explorer/Outlook

Per installare Internet Explorer/Outlook, andare su <http://www.microsoft.com>. Seguire le istruzioni onscreen per effettuare il download ed installare il pacchetto.

### Mozilla Firefox

Per installare Internet Explorer/Outlook, andare su <http://www.mozilla.com/>. Seguire le istruzioni onscreen per effettuare il download ed installare il pacchetto.

<sup>1</sup>Indirizzo web corretto al momento della pubblicazione del manuale.

## CAPITOLO 7 – USO DEL BIT4ID Middleware Universale


Nel presente capitolo sono trattati i seguenti aspetti:

- Avvio e chiusura del BIT4ID Middleware Universale
- Esportazione certificato
- Accesso alle informazioni della carta
- Cambio del PIN di login
- Cambio del PIN di firma
- Sblocco del PIN di login
- Sblocco del PIN di firma

### Avvio e chiusura del BIT4ID Middleware Universale


Quando la procedura di installazione è stata completata, selezionare **Start / Programs / Bit4id / Bit4id – Smart Card Manager**



A questo punto l'applicazione gira in background e appare l'icona  nel system tray (pannello a sinistra dell'orologio).

#### Avvio

Per avviare BIT4ID Middleware Universale, procedere come segue:

4. Inserire la carta CNS nel lettore.
5. Cliccare con il tasto destro l'icona  e selezionare CNS Manager. Il lettore legge la carta e appare la finestra di login.
6. Inserire il pin di login e cliccare il pulsante Log in.

### Finestra Principale - Illustrazione

Dopo aver inserito il pin di login, appare la seguente finestra principale:




## Finestra Principale – Descrizione

La finestra principale comprende quattro tabs come descritto sotto:

| Tab                | Descrizione   |
|--------------------|---|
| Informazioni       | Fornisce le informazioni sulla smart card.  |
| Cambio PIN         | Consente di cambiare il proprio PIN di login. Per ulteriori dettagli, si veda il paragrafo intitolato <a href="#">Cambio del PIN di Login</a> a pagina 6. |
| Sblocca smart card | Consente di sbloccare la carta inserendo il PUK.  |
| Avanzate           | Opzioni avanzate  |

## Uscita

| Se si vuole...  | Si deve...   |
|---|--|
| Uscire dalla finestra principale, ma lasciare CNS Manager nel system tray | Cliccare la crocetta nell'angolo in alto a destra della finestra.  |
| Chiudere BIT4ID Middleware Universale                                     | Fare click con il tasto destro sull'icona  in basso a destra del vostro schermo e selezionare uscita. |

## Accesso Informazioni sulla carta

Questa sezione descrive come accedere alle informazioni sulla smart card. Le seguenti informazioni sono disponibili, come descritto sotto:

| Campo (Field)     | Definisce...                             |
|-------------------|--|
| Numero di serie   | Numero di serie della vostra smart card  |
| Etichetta/Modello | Nome/Modello della smart card inserita   |
| Produttore        | Estremi del produttore della smart card. |
| Lunghezza del PIN | Vincoli sulla lunghezza del codice PIN.  |
| Memoria libera    | Memoria disponibile in bytes.            |
| Letto in uso      | Informazioni sul lettore in uso.         |

### Procedura

Per accedere alle informazioni sulla smart card, entrare in CNS Manager come descritto nel paragrafo a pagina relativo.

Apparirà automaticamente il tab **Informazioni** sulla finestra principale.



## Cambio del PIN di login

Per cambiare un PIN, si proceda nel modo seguente:

7. Aprire la finestra principale come descritto precedentemente
8. Cliccare il tab **Cambio PIN**.

Appare la finestra sottostante:

The screenshot shows a software window titled "4 Bit4id - Middleware Universale". The window has a blue header bar with the "UNIVERSAL MW4" logo on the left and the "Oberthur Card Systems" logo on the right. Below the header, there is a tabbed interface with five tabs: "Smart card", "Cambio PIN", "Sblocca smart card", "Avanzate", and "Inform". The "Cambio PIN" tab is currently selected and highlighted. The main area of the window contains three text input fields: "Vecchio PIN:", "Nuovo PIN:", and "Conferma nuovo PIN:". At the bottom right of the form area, there is a blue button with the text "ESEGUI" and a right-pointing arrow.

9. Inserire il PIN attuale nel campo **Vecchio PIN**.
10. Inserire il nuovo PIN nel campo **Nuovo PIN**.
11. Confermare il nuovo PIN nel campo **Conferma nuovo PIN**.
12. Cliccare **ESEGUI**.  
Il nuovo PIN è stato applicato. Da questo momento dovrà essere utilizzato per effettuare il log in.

## Sblocco del PIN di Login

Nel caso in cui si sbagliasse per tre volte consecutive l'immissione del PIN di Login, per ragioni di sicurezza, la smart card blocca il PIN di login e il relativo accesso. Per sbloccare il PIN di login è necessario immettere un codice di sblocco chiamato PUK.

The screenshot shows a software window titled "Bit4id - Middleware Universale". The interface includes a header with the text "UNIVERSAL MW<sup>4</sup>" and the "Oberthur Card Systems" logo. Below the header is a navigation bar with tabs: "Smart card", "Cambio PIN", "Sblocca smart card" (which is currently selected), "Avanzate", and "Inform". The main area contains three text input fields labeled "PUK:", "Nuovo PIN:", and "Conferma nuovo PIN:". At the bottom right of the main area is a blue button labeled "ESEGUI" with a right-pointing arrow.

Per sbloccare il PIN, procedere come segue:

6. Digitare il PUK della carta CNS nella casella di testo **PUK**
7. Digitare un nuovo PIN nella casella di testo Nuovo PIN
8. Ridigitare il PIN appena immesso nella casella di testo Conferma nuovo PIN
9. Cliccare sul pulsante Esegui
10. Un messaggio conferma l'avvenuto sblocco del PIN di Login

**ATTENZIONE:** Immettendo un PUK errato per tre volte consecutive, il PIN di Login viene definitivamente e irreversibilmente bloccato.



## CAPITOLO 8 – USO DEL WEB BROWSER con BIT4ID Middleware Universale

In questo capitolo sono contenute tutte le informazioni necessarie per leggere il certificato sul browser e per firmare o cifrare e-mail in combinazione con CNS Manager.

### Argomenti Principali

In questo capito sono trattati i seguenti argomenti:

- Lettura del certificato con Internet Explorer
- Autenticazione Web

### Requisiti Tecnici

Sono richieste le seguenti versioni di browser e mailer:

- Internet Explorer 5.0 o successive e Outlook 2000 o Express
- Mozilla Firefox o successivi

### Configurazione del Browser

#### Internet Explorer

Non è necessario fare nulla.

#### Mozilla FireFox

In questo paragrafo viene descritta la procedura da seguire per impostare Mozilla FireFox in modo che legga automaticamente i certificati contenuti nella CNS smart card. Procedere come segue:

6. Avviare Mozilla FireFox
7. Selezionare Opzioni File dal menu Strumenti
8. Selezionare Avanzate
9. Selezionare Cifratura
10. Selezionare Dispositivi di sicurezza
11. Cliccare su Carica
12. Nella finestra che si e' aperta cliccare su Sfoglia
13. Entrare nella cartella C:\WINDOWS\system32 e selezionare il file bit4opki.dll
14. Fare click su apri
15. Cliccare su OK ai messaggi che si presenteranno nel seguito

Volendo ripristinare la configurazione originale,procedere come segue:

1. Avviare Mozilla FireFox
2. Selezionare Opzioni File dal menu Strumenti
3. Selezionare Avanzate
4. Selezionare Cifratura
5. Selezionare Dispositivi di sicurezza
6. Selezionare Nuovo Modulo PKCS#11
7. Selezionare Scarica
8. Cliccare su OK ai messaggi che si presenteranno nel seguito

### Lettura dei Certificati

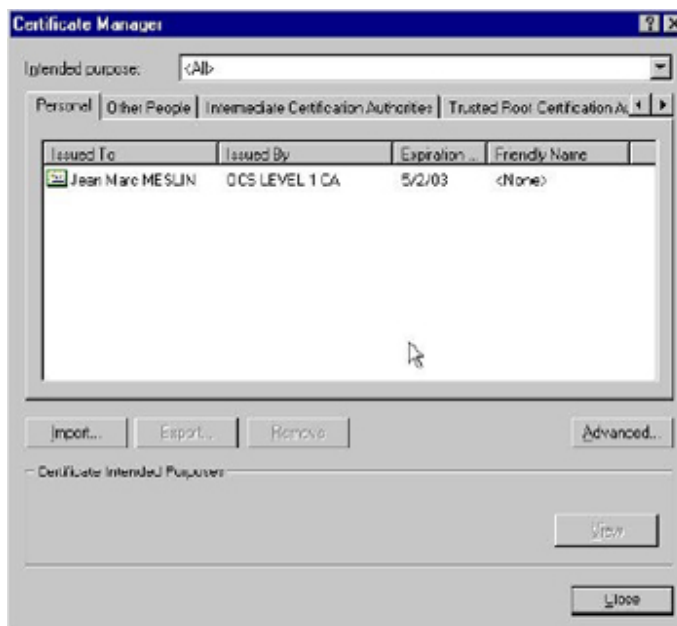
Questa sezione indica come leggere il certificato una volta che è stato installato sul browser. Non è necessaria una configurazione

per Internet Explorer. Lo si può utilizzare per effettuare in sicurezza operazioni online.

## Internet Explorer

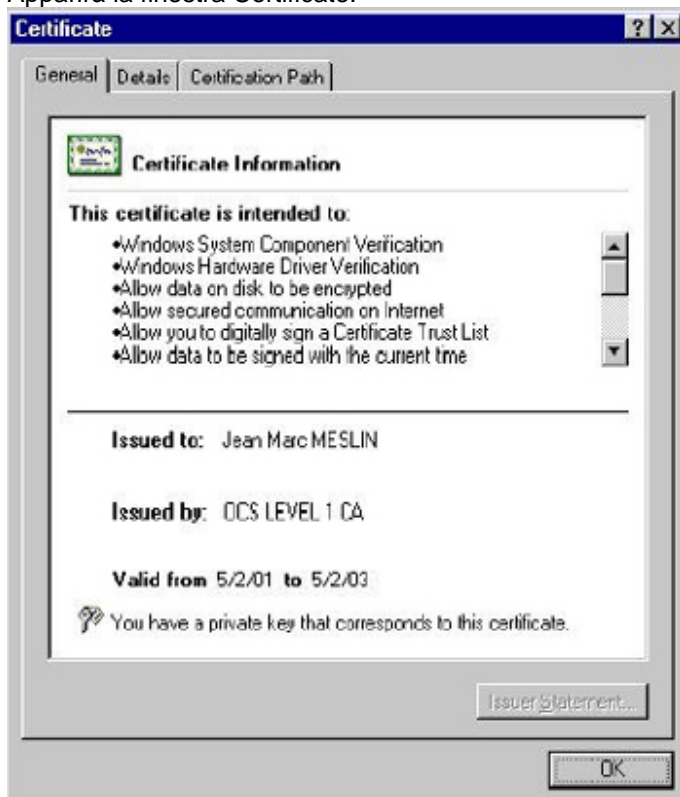
Per poter leggere un certificato su Internet Explorer, si proceda nel modo seguente:

8. Inserire la smart card CNS nel lettore.
9. Avviare Internet Explorer.
10. Nel menu **Strumenti**, cliccare **Opzioni Internet**.
11. Cliccare il tab **Contenuto**
12. Nell'area **Certificati**, cliccare il pulsante **Certificati** per vedere i certificati installati.  
Apparirà la finestra **Certificate Manager**:



13. Selezionare il certificato e cliccare View.

Apparirà la finestra Certificate:



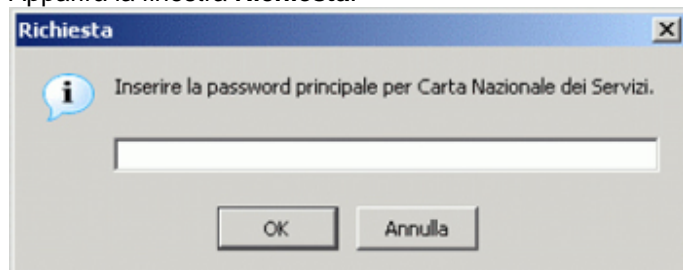
14. Cliccare OK, e, una volta terminato il tutto, Close.

## Mozilla FireFox

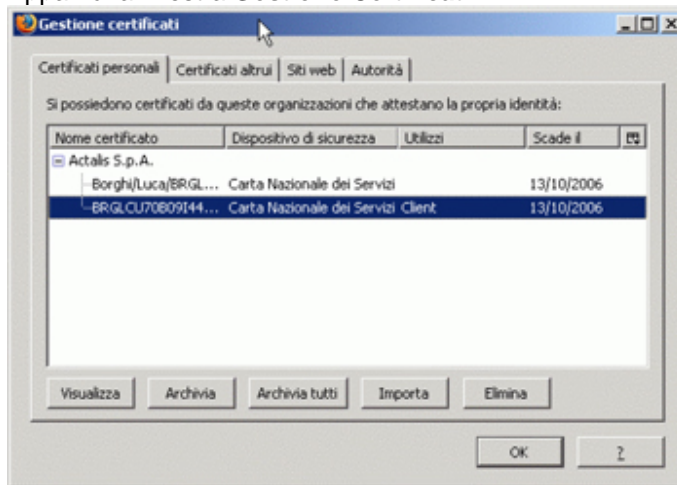
Per poter leggere un certificato su Mozilla FireFox, si proceda nel modo seguente:

11. Inserire la smart card CNS nel lettore.
12. Avviare Mozilla FireFox.
13. Selezionare **Strumenti, Opzioni**
14. Selezionare la sottofinestra **Avanzate**
15. Cercare la sezione **Certificati**
16. Cliccare sul pulsante **Gestione Certificati**

Apparirà la finestra **Richiesta**:



- Inserire il PIN di Login e cliccare **OK**.  
Apparirà la finestra **Gestione Certificati**:



- Selezionare il tab **Certificati personali**.
- Cliccare con il tasto sinistro sul certificato corrispondente per selezionarlo e cliccare il pulsante **Visualizza**. Apparirà una descrizione dettagliata del certificato
- Cliccare **OK** per chiudere

## Autenticazione WEB

La CNS smart card dispone di certificati che permettono l'autenticazione WEB. Normalmente i dati scambiati via internet sono "in chiaro" e un intruso potrebbe indebitamente accedere a informazioni confidenziali. E' possibile, tramite il protocollo SSL (Secure Socket Layer), stabilire un canale di comunicazione criptato e sicuro.

Oltre a questo primo livello di sicurezza, l'autenticazione web è un meccanismo che, grazie alla smart card CNS, permette al server web di assicurarsi dell'identità dell'utente che cerca di connettersi. Le informazioni riservate comunicate dal server web saranno protette per due ragioni:

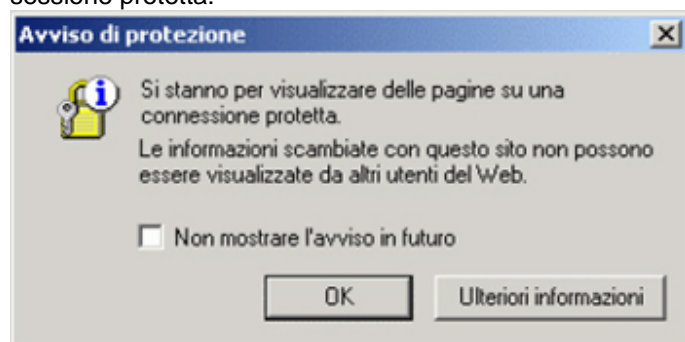
3. Sono criptate e firmate, quindi nessuno può né leggerle né modificarle
4. Sono trasmesse solo se l'utente è stato validamente identificato

IMP: Se non si importano i certificati delle certification authorities che hanno emesso il proprio certificato, il browser non permette l'uso dei certificati SSL client.

Qui di seguito la procedura da seguire per autenticarsi su richiesta di un server web che voglia stabilire una sessione SSL.

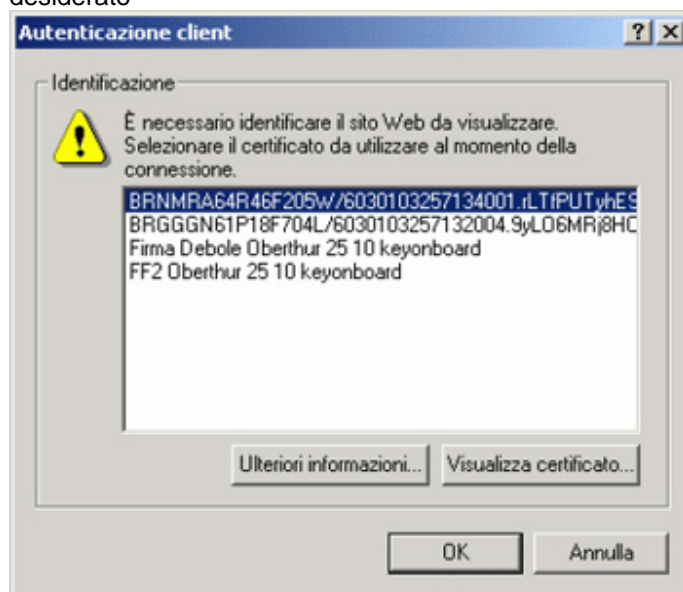
## Internet Explorer

Aperto una connessione sicura con un server web, Explorer avverte che si sta per aprire una sessione protetta:



Seguire la procedura specificata qui di seguito:

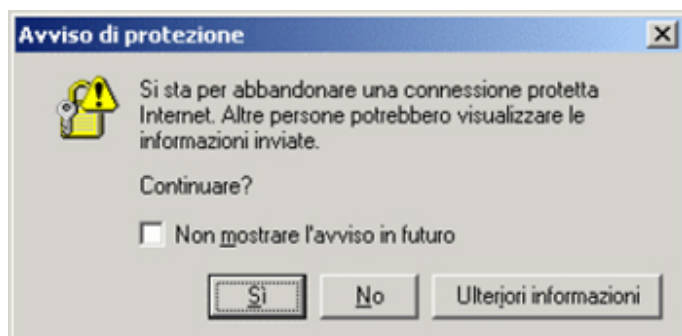
5. Cliccare su **OK**
6. Apparirà la finestra di **Autenticazione Client** dove poter scegliere il certificato di autenticazione desiderato



7. Scegliere il certificato di autenticazione desiderato e cliccare **OK**  
Apparirà la finestra di **Avviso di protezione**
8. Cliccare su **Si** (solo se la data del certificato è valida)

Da questo momento in avanti la connessione è sicura, cioè nessuno potrà leggere i dati intercorrenti tra server e client. Internet Explorer segnala lo stato di connessione sicura visualizzando nella sua status bar.

Terminando la connessione sicura, Microsoft Explorer visualizzerà la seguente finestra che avvisa il cambiamento di stato di connessione.

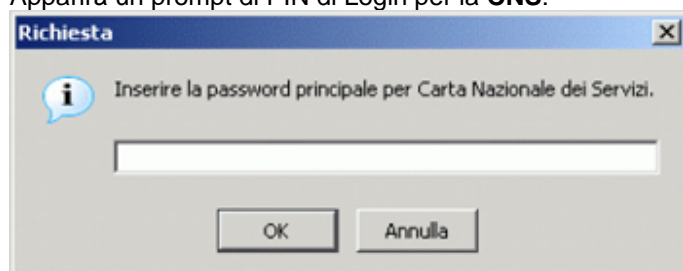


### Mozilla FireFox

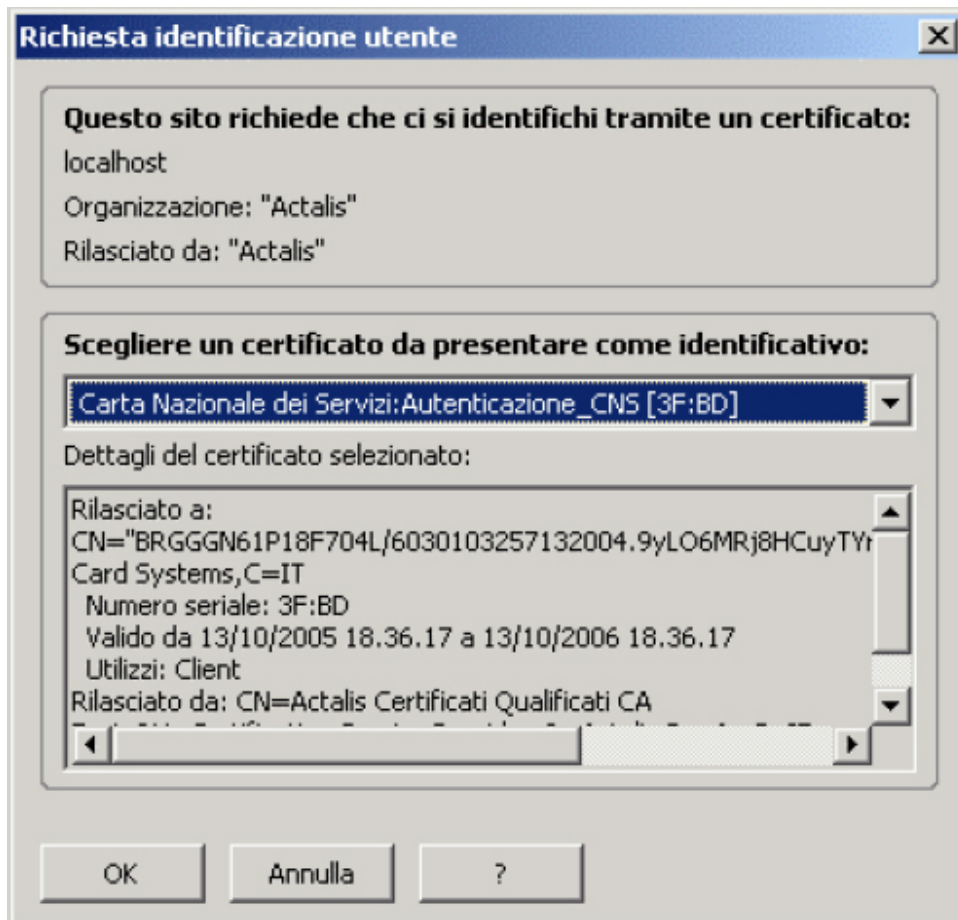
Aperto una connessione sicura con un server web, Mozilla FireFox avverte che si sta per aprire una sessione protetta.

Seguire la procedura specificata qui di seguito:


5. Apparirà un prompt di PIN di Login per la **CNS**:



6. Inserire il PIN di Login e cliccare su **OK**
7. Apparirà la finestra di **Richiesta identificazione Utente** dove poter scegliere il certificato di autenticazione desiderato



8. Scegliere il certificato di autenticazione desiderato e cliccare **OK**

Da questo momento in avanti la connessione è sicura, cioè nessuno potrà leggere i dati intercorrenti tra server e client. Mozilla FireFox segnala lo stato di connessione sicura visualizzando  nella sua status bar e ombreggiando in giallo la barra degli indirizzi.

## DOMANDE FREQUENTI

### Explorer non visualizza i certificati presenti sulla carta. Cosa faccio?

Probabilmente la libreria che gestisce la sincronizzazione dei certificati sullo store di Windows è in uno stato incoerente con lo stato della carta. Per ripristinare la correttezza degli stati, bisogna rilanciare i servizi che si occupano della sincronizzazione. Procedere come segue:

1. Estrarre la carta dal lettore
2. Chiudere Explorer
3. Premere "Ctrl-Alt-Canc" e selezionare "Task Manager"
4. Selezionare il tab "Processi"
5. Selezionare il processo "OcsCertSynchronizer"
6. Cliccare sul pulsante "Termina processo"
7. Rispondere "Sì" all'avviso che verrà visualizzato
8. Selezionare il processo "AuthManagerV3"
9. Cliccare sul pulsante "Termina processo"
10. Rispondere "Sì" all'avviso che verrà visualizzato
11. Chiudere il "Task manager"
12. Aprire il "Pannello di controllo"
13. Aprire gli "Strumenti di Amministrazione"
14. Aprire "Servizi"
15. Selezionare "Oberthur Cryptolib Services"
16. Riavviare il servizio con l'apposito pulsante nella barra dei pulsanti
17. Riavviare il Synchroniser in C:\Windows\, file OcsCertSynchronizer.exe
18. Riavviare il "CNS Manager" dal menu "Avvio"

Se neanche in questo modo il problema si risolve, riavviare la macchina.

Se il problema persiste, contattare il Call center della Carta Nazionale dei Servizi.

### Qual è il nome dell'eseguibile corrispondente al "CNS Manager"

L'eseguibile si trova in "C:\WINNT\" e si chiama "AuthManagerV3.exe"

### Qual è la directory di installazione del CNS Manager

La directory di installazione di default è "C:\Programmi\CNS Manager" dove si possono trovare questo manuale in forma elettronica e i due file di configurazione per Mozilla (v. pag. 10)

### Mozilla non visualizza i certificati presenti sulla carta. Cosa faccio?

Molto probabilmente la mozilla non è stato configurato correttamente. Per configurare mozilla far riferimento al capitolo corrispondente del presente manuale.



## GLOSSARIO

### Autenticazione

L'autenticazione verifica l'identità delle entità che comunicano in rete. Permette di aprire un canale sicuro (SSL) tra l'utente e il server che offre un servizio in rete.

L'utilizzo di una SmartCard (come la Carta Nazionale dei Servizi) aggiunge ulteriore sicurezza al processo in quanto:

1. E' necessario essere in possesso della Smart card
2. E' necessario conoscere il PIN di login
3. Non è possibile estrarre dalla Smart Card le chiavi utilizzate per aprire il canale sicuro

### Certificato

Documento digitale comunemente utilizzato per l'autenticazione e lo scambio di informazioni in sicurezza nei networks aperti, come Internet, Extranets ed Intranets. Un certificato lega con certezza una chiave pubblica all'entità che possiede la corrispondente chiave privata. I Certificati hanno la firma digitale della Certification Authority emittente e possono essere emessi per un utente, un computer o un servizio. Il formato comunemente accettato è definito standard internazionale ITU-T X.509 versione 3.

### Certification Authority (CA)

Entità responsabile di stabilire e di garantire l'autenticità delle chiavi pubbliche appartenenti agli utenti (e alle entità) o alle altre certification authorities. L'attività di una certification authority può comprendere: vincolare chiavi pubbliche a nomi distinti tramite certificati firmati, gestione dei numeri seriali dei certificati, revoca dei certificati.

### Decifratura

Contrario della corrispondente cifratura. Operazione realizzata per rintracciare il messaggio originale utilizzando una chiave simmetrica segreta o una chiave privata asimmetrica. Si veda anche Cifratura.

### Firma Digitale

Trasformazione crittografica irreversibile di dati che permette al destinatario di tali dati di verificarne l'origine e l'integrità; protegge mittente e destinatario da falsificazioni da parte di terzi e protegge il mittente da falsificazioni da parte del destinatario.

### Cifratura

Trasformazione reversibile di dati tramite un algoritmo crittografico con lo scopo di generare un crittogramma; la cifratura può essere realizzata utilizzando una chiave simmetrica o asimmetrica. Si veda anche Decifrazione.

## Extranet

Sottoinsieme limitato di computer o utenti in una rete pubblica, tipicamente Internet, che possono accedere alla rete interna di una organizzazione. Tipicamente i computer o gli utenti appartenenti a organizzazioni partner.

## Intranet

Rete di computer interna ad una organizzazione disponibile esclusivamente ai dipendenti dell'azienda. Una intranet è chiamata anche rete privata.

## Non ripudio

Funzione basilare di sicurezza in crittografia. Il "non ripudio" assicura che un interlocutore non possa negare proditoriamente che la comunicazione (o una sua parte) sia avvenuta. Senza il "non ripudio", qualcuno potrebbe comunicare qualcosa e poi negare di averlo fatto o affermare di averlo fatto in un altro momento.

## Chiave privata

É la parte segreta di una coppia di chiavi crittografiche usate negli algoritmi a chiave pubblica. Le chiavi private sono tipicamente utilizzate per firmare digitalmente o per decriptare dati che sono stati criptati con la corrispondente chiave pubblica. Vedere anche Chiave Pubblica

## Chiave pubblica

É la parte non segreta di una coppia di chiavi crittografiche usate negli algoritmi a chiave pubblica. Le chiavi pubbliche sono tipicamente utilizzate per verificare le firme digitali o per decriptare dati crittografati con la corrispondente chiave privata. Vedere anche Chiave Privata

## Algoritmo a chiave pubblica

Algoritmo di cifratura asimmetrica che usa due chiavi, una pubblica per la codifica, una private per la decodifica.

## RSA

RSA è un acronimo che si riferisce all'algoritmo a chiave pubblica inventato da Ron Rivest, Adi Shamir e Leonard Adleman e brevettato dalla loro società, RSA Data Security.

L'algoritmo a chiave pubblica RSA è stato adottato per diversi tipi di codifica, dalla firma digitale all' SSL (Secure Sockets Layer) usato per proteggere le trasmissioni tra web browsers e web servers

## Smart Card

Sono dei dispositivi simili ad una carta di credito, dotati di un chip sofisticato che permettono, dietro l'immissione di un PIN, l'autenticazione tramite un certificato.

Le smart card immagazzinano in modo sicuro certificati, chiavi pubbliche e private, password e altri tipi di informazioni personali. Un lettore può essere collegato al computer per leggere le smart card.